

TASK ORDER

47QFCA18F0122

Responsive Environment for Agile Counterterrorism Solutions (REACTS)

in support of:

The Office of the Director of National Intelligence (ODNI) / National Counterterrorism Center (NCTC)



Awarded to:

**Leidos Innovations Corporation
under
Alliant Governmentwide Acquisition Contract (GWAC) Number GS00Q09BGD0039**

Issued by:

**The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405**

**Award Date: September 27, 2018
Modification PO-03 Date: January 28, 2019
FEDSIM Project Number IO00900**

SECTION J - ATTACHMENTS

C.1 BACKGROUND

The Office of the Director of National Intelligence (ODNI)/ National Counterterrorism Center (NCTC) requires the establishment of a new Development Operations (DevOps) enabled Responsive Environment for Agile Counterterrorism Solutions (REACTS). The DevOps enabled REACTS shall support mission-driven Information Technology (IT), Infrastructure Solutions and Services, and Commodity Support.

The NCTC has the responsibility to:

- a. Effectively operate and maintain the NCTC mission critical counterterrorism (CT) IT applications and systems while continually, incrementally, and rapidly enhancing their capabilities.
- b. Deliver the information required to detect, deter, and counter terrorist activities and plans while maintaining the confidentiality, integrity, and availability of that data.
- c. Deploy new and improve current IT tools and systems that strengthen and integrate core analytic and other mission capabilities, provide an integrated business application framework for interoperability and technology re-use, and maximize IT investments to improve mission performance.
- d. Develop an integrated IT system that enables collaboration, data use, data exploitation, and information sharing within the NCTC and across the CT community.
- e. Meet compliance and reporting requirements as specified by various policies and oversight bodies.

C.1.1 PURPOSE

NCTC has four primary priorities for provision of IT services: agility, innovation, availability 24 hours per day/seven days per week/365 days per year (24/7/365), and delivery at the speed of mission. NCTC prioritizes these same attributes in its management of the data life cycle in addition to access to Proof of Concept or rapid prototyping and compliance with statutory and policy requirements. These IT services are provisioned and implemented for the sole purpose of supporting mission and mission support elements to enable efficient, robust, and timely conduct of NCTC responsibilities. Enterprise-wide infrastructure capability requirements coupled with, mission element requirements guide IT prioritization and implementation efforts. A thorough understanding of mission activities and needs is imperative to leverage technology design, development, capabilities, and integration to adequately maintain existing tools and provide new capabilities that enhance effectiveness.

The purpose of this TO is to design, develop, implement, and maintain an IT environment that will provide the stability and flexibility the NCTC requires to meet mission needs and support other mission partners. In particular, the NCTC requires a DevOps execution model that integrates services, hardware, software, and/or data support; incorporates new sources; maintains ingestion services as formats/schemas change; improves throughput and efficiency; develops and deploys self-service tools to exploit and use data more quickly, thoroughly, and robustly; and manages compliance requirements as may be necessary to satisfy CT service, application, tool, data, and other IT mission needs across the NCTC. This requirement includes Project Management, establishment of a DevOps ecosystem, and Agile innovation development

SECTION J - ATTACHMENTS

capabilities to enable the continuous delivery of functioning services and products, to meet the needs of the mission user, as priorities change and new data becomes available.

C.1.2 AGENCY MISSION

The NCTC's role as the primary organization in the United States Government (Government) for analyzing and integrating CT intelligence possessed and acquired by the Government requires a flexible and responsive IT environment to quickly meet evolving and changing mission priorities. NCTC's technology services, infrastructure, and development must provide daily and ongoing support to mission elements tasked with conducting statutory responsibilities to counter terrorism. Mission operations include strategic and tactical intelligence analysis and integration; screening, vetting, and watchlisting; situational awareness; and strategic planning.

C.2 SCOPE

This TO will be performed in the Washington Metropolitan Area and will integrate the acquisition, development, delivery, oversight, and control of mission enabling IT; implement a DevOps execution model that integrates services, hardware, software, and/or data support; incorporates new sources; maintain ingestion services as formats/schemas change; and improve throughput and efficiencies. This TO will provide a new enterprise-wide DevOps environment that develops next generation capabilities while integrating existing functional requirements. NCTC's intent is to provide maximum flexibility to the contractor to provide a transformational solution that integrates and accelerates the provision of IT and data services. NCTC is committed to partnering with the contractor; modifying and re-engineering its existing internal structures and business and governance processes, and enabling implementation of the contractor's solution. NCTC is also positioned to partner with relevant NCTC security elements to increase the efficiency of the onboarding process for contracting staff and deliver rapid Authorization to Operate (ATO) to support continuous DevOps cycles.

This TO will provide Project Management, and DevOps enabled technical and management services, hardware, software, data ingestion, maintenance, data exploitation, infrastructure, innovation, compliance, mission integration, and security to support:

- a. Responsive IT engineering and development to address dynamic and fast-paced mission needs.
- b. The full lifecycle of the NCTC planning, acquisition of approved components and services, implementation, operations, enhancement, sustainment, and retirement of legacy IT systems, data, and infrastructure as the NCTC moves towards Intelligence Community (IC) Information Technology Enterprise (ITE) Cloud Services.
- c. Innovation and analytic capability advancements to keep pace with rapidly emerging and changing terrorist activities and methodologies.
- d. Enhancing IT systems, data, and infrastructure (including services) as new data sources arrive, missions evolve, and leading edge technologies become available.
- e. Establishing a DevOps execution model and transitioning current system and service support to the new model.
- f. Using data science techniques and tools to meet evolving mission requirements.
- g. Using IC ITE common services to reduce redundancy, increase efficiencies, and improve integration and collaboration across the IC.

SECTION J - ATTACHMENTS

- h. Applying a cloud-first approach for the NCTC IT services including the development and migration of data, infrastructure, and applications into a cloud environment. New services and systems shall take a cloud-first approach (not necessarily a lift-and-shift model) focused on migrating to existing Government-furnished cloud platforms while remaining flexible for a hybrid solution.
- i. Completing software development using Agile engineering and development methods. The contractor shall leverage Agile processes to provide a mechanism for computing the priority of work to be completed (the product backlog) and determining software acceptance (user story acceptance criteria). Agile methods shall conform to the broad definition of Agile Engineering Best Practices.
- j. Employing and leveraging the Information Technology Infrastructure Library (ITIL) Service Management Framework (Version 3 and any subsequent revisions) to guide provisioning of services, processes, functions, and other capabilities needed to support them.
- k. Employing and leveraging the principles and practices of the Project Management Body of Knowledge (PMBOK)TM to execute enterprise project management for the TO. The contractor may recommend alternate procedures to the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer Representative (COR) and NCTC Technical Point of Contact (TPOC) if it believes other (Proprietary or Open) processes or procedures are equivalent or better.
- l. Applying an approved governance process for management of the NCTC mission IT product development, deployment, and maintenance.
- m. Executing and monitoring the effectiveness of the NCTC IT policy, compliance, and baseline processes; providing status to the Government; and recommending adjustments in order to improve IT performance, shorten timelines, reduce burden, promote innovative development, and increase mission value.
- n. Working collaboratively across the NCTC organizations and with the other NCTC contractor support to develop, coordinate, and execute IT plans addressing current and evolving mission priorities, technology opportunities, and longer term objectives.
- o. Supporting and/or participating in technical exchange meetings (TEMs), working groups, boards, committees, teams, and other NCTC forums.
- p. Engaging mission elements to identify, develop, and implement technology, innovation, and methodological innovation and analytic advancements.

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

The NCTC, staffed by Government personnel from more than 30 different departments and agencies, is a center for the production of analysis, maintenance of the authoritative database of known and suspected terrorists, information sharing, and strategic operational planning. The NCTC is the primary organization in the Government for analyzing and integrating all intelligence possessed or acquired by the Government pertaining to terrorism and CT except intelligence pertaining exclusively to domestic terrorism. This involves the exploitation of large quantities of data including many different data types, from many different data providers of varying velocity that need to be ingested, integrated, stored, processed, analyzed, turned into

SECTION J - ATTACHMENTS

information products, and rapidly disseminated to IC, Department of Defense (DOD), and other Governmental partners to meet critical mission needs.

NCTC also has the statutory responsibility to serve as the central and shared knowledge bank on known and suspected terrorists and international terror groups and to ensure other mission partners have access to and receive intelligence to accomplish assigned missions. This involves a significant technical effort to curate, analyze, and make this information and associated insights available to internal and external users. The Government's supporting technical environment includes the infrastructure, data platforms, and processing to operate and maintain mission services, analytics, applications, tools, and knowledge repositories; provide correlation services and big data analytics; and enable coordination and collaboration with mission users across the Government.

The Government's infrastructure currently runs on five different and independent networks, where the majority of implementation and engineering activities occur. The Government is in the process of migrating applications to the cloud. The Government also maintains a limited amount of hardware and network connections inside the Government's enclaves and to other external mission partners.

Much of this infrastructure is being moved to a Government cloud environment and the majority of all servers are virtualized. The Government is using an enclave approach for hosting IT and information systems, and each environment has a similar configuration with directory services, central audit services, system management tools, network configuration, and storage configuration. Enclaves are separated by classification level and use common components and services that may be hosted and managed internally, or in an internal or external Government-controlled cloud environment.

Additional information for the current IT/Network Environment is provided in Section J, Attachment Y.

C.3.1 NOTIONAL REACTS CONCEPT OF OPERATIONS (CONOPS)

The REACTS CONOPS enables the Government and the contractor to create and resource multi-functional teams to support mission portfolios and develop new mission-focused capabilities using an Agile methodology.

Current and future mission needs are decomposed into prioritized high-level concepts and functional requirements. These requirements are further transformed into prioritized acquisition-ready tasks that are allocated to Task Backlogs and then executed. The CONOPS graphic below provides a generic depiction of the notional future state for the NCTC CONOPS.

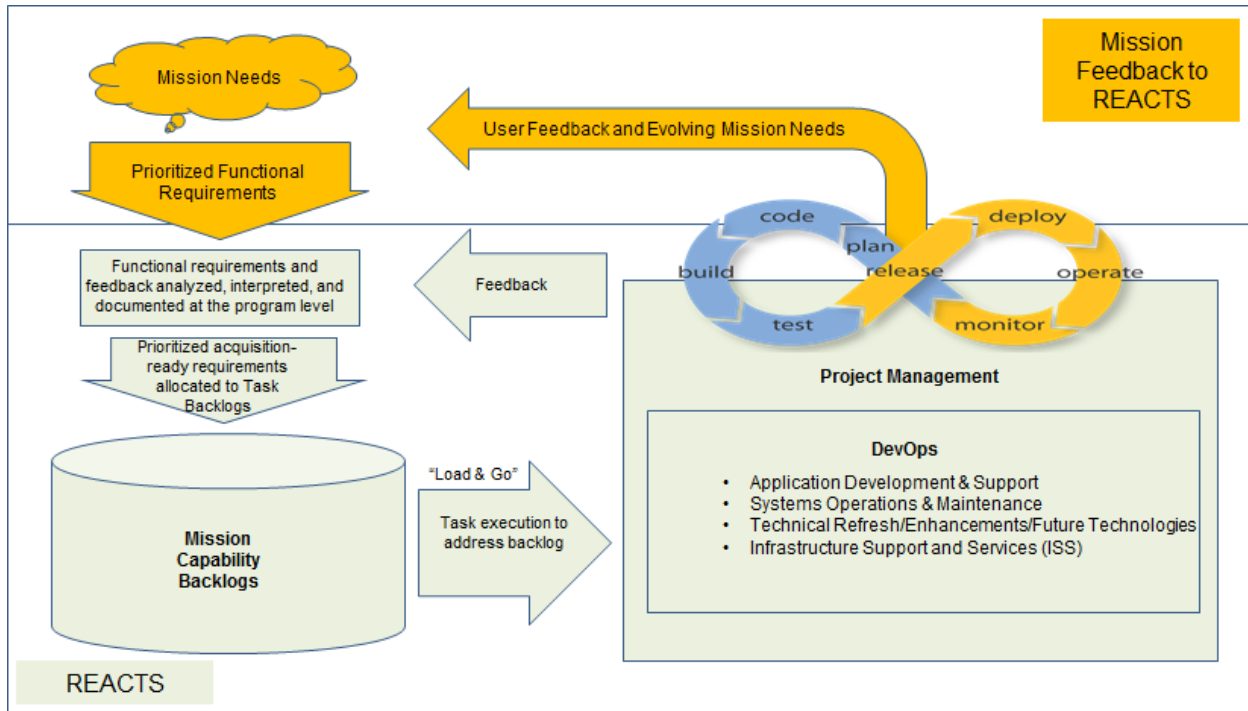


Figure 1: Notional REACTS DevOps CONOPS

C.3.2 COUNTERTERRORISM (CT) SERVICES, APPLICATIONS, AND TOOLS

The overarching vision as defined in the REACTS DevOps CONOPS will guide development and deployment of CT capabilities, advancements, services, applications, and tools. These capabilities will provide a mission-centric, collaborative, data-driven, task-oriented, innovative and technologically-exploitative environment to support mission operations.

Existing and required CT services, applications, and tool capabilities are identified in the NCTC Target Architecture Service Reference Model (provided at TO award).

C.4 OBJECTIVE

The contractor shall create an integrated IT solution that will fulfill all of the requirements and manage an integrated ITE solution that will fulfill infrastructure requirements. The contractor shall support the transition or retirement of existing systems and ensure those system requirements are embedded in the new system if essential to support continuing mission needs. The following functional areas will be transitioned to the REACTS TO: data correlation, workflow, screening, Operations and Maintenance (O&M), rapid innovation and prototyping, prototype movement to enterprise-wide capabilities, legacy application/system mission capability enhancements, infrastructure, security, e-mobility, web applications, metrics, compliance-related audit, and Disaster Recovery (DR).

The contractor shall provide a solution to meet the task requirements below, as well as a solution that will meet the future and rapidly advancing requirements as the environment evolves and changes. This solution includes, but is not limited to, modifying, changing, advancing, replacing, supplementing, enhancing, and decommissioning the included CT services, applications, tools, and other supporting capabilities over time with rapid development and implementation.

SECTION J - ATTACHMENTS

The Government will make every effort to give the contractor 60 to 90 days advance notice of new requirements, but the dynamic and unpredictable nature of the NCTC environment dictates that emergent requirements can and will occur with little or no advance notice. The contractor shall be prepared to respond rapidly to such requirements as they are identified throughout the course of performance. The contractor shall be flexible as the portfolio of projects, team size, and skills required may change regularly due to mission customer requirements, NCTC priorities, or budget adjustments. The contractor shall modify and scale its staff to ensure that an adequate number of resources with the appropriate skill mix are deployed in order to effectively adapt to the changes that may occur throughout the life of the REACTS TO.

The contractor shall be prepared to support National Security events that are unplanned and unknown under Task 6, Provide Additional REACTS Response Support. The contractor shall respond to a Government request to meet circumstances of a critical National Security nature. These requests may require a response to an emerging situation that requires a new capability and/or rapid augmentation of an existing capability. The contractor shall deliver all source code, scripts, documentation, datasets, etc. that have been modified in support of this task and ensure all such materials comply with the security standards.

Interoperability between NCTC systems and partner systems and datasets is imperative.

C.5 TASKS

- a. Task 1 – Provide Project Management Support
- b. Task 2 – Provide Transition Support
- c. Task 3 – Development Support
- d. Task 4 – Systems O&M Support
- e. Task 5 – Data Management
- f. Task 6 – Provide Additional REACTS Response Support (Optional)

C.5.1 TASK 1 – PROVIDE PROJECT MANAGEMENT SUPPORT

The contractor shall provide project management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The contractor shall identify a Project Manager (PM) by name that shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

C.5.1.1 SUBTASK 1.1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at the location approved by the Government (Section F, Deliverable 03). The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include contractor Key Personnel, representatives from the directorates, other relevant Government personnel, and the FEDSIM COR.

SECTION J - ATTACHMENTS

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (Section F, Deliverable 02) for review and approval by the FEDSIM COR and the NCTC TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

- a. Points of contact (POCs) for all parties
- b. Draft Project Management Plan (PMP) (Section F, Deliverable 08) and discussion including schedule, tasks, etc.
- c. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government).
- d. Staffing Plan and status.
- e. Updated Transition-In Plan (Section F, Deliverable 15) and discussion
- f. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs)).
- g. Invoicing requirements
- h. Updated Baseline Quality Control Plan (QCP) (Section F, Deliverable 12)

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a Kick-Off Meeting Minutes Report (Section F, Deliverable 04) documenting the Kick-Off Meeting discussion and capturing any action items.

C.5.1.2 SUBTASK 1.2 – PREPARE A WEEKLY STATUS REPORT (WSR)

The contractor shall develop and provide a WSR (Section F, Deliverable 27). The WSR shall include the following:

- a. Personnel gains, losses, and status (security clearance, etc.), including close out activities as required by the NCTC.
- b. Progress updates and demonstrations.
- c. TO schedule updates.
- d. Government actions required.
- e. Sprint Schedule (Sprint Backlog, planned, actual, and completion dates for each sprint)

C.5.1.3 SUBTASK 1.3 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR (Section J, Attachment F) (Section F, Deliverable 05). The MSR shall include the following:

- a. Activities during reporting period, by task (include on-going activities, new activities, and activities completed, and progress to date on all above mentioned activities). Each section shall start with a brief description of the task.
- b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- c. Government actions required.
- d. Schedule (show major tasks, milestones, and deliverables; planned, actual, and completion dates for each).

SECTION J - ATTACHMENTS

- e. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).
- f. Accumulated invoiced cost for each CLIN up to the previous month.
- g. Projected cost of each CLIN for the current month.

C.5.1.4 SUBTASK 1.4 – CONVENE TECHNICAL STATUS MEETINGS

The contractor PM shall convene a Monthly Technical Status Meeting with the NCTC TPOC, FEDSIM COR, and other Government stakeholders (Section F, Deliverable 06). The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities and ensure that captured requirements meet mission needs. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the FEDSIM COR within five workdays following the meeting (Section F, Deliverable 07).

C.5.1.5 SUBTASK 1.5 – PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The contractor shall provide the Government with a draft PMP (Section F, Deliverable 08) on which the Government will make comments. The final PMP (Section F, Deliverable 09) shall incorporate the Government's comments.

The PMP shall:

- a. Describe the proposed management approach.
- b. Contain detailed Standard Operating Procedures (SOPs) for all tasks.
- c. Include milestones, tasks, and subtasks required in this TO.
- d. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations.
- e. Describe in detail the contractor's approach to risk management under this TO.
- f. Describe in detail the contractor's approach to communications, including processes, procedures, communication approach, and other rules of engagement between the contractor, the Government, and other contractors at the enterprise level.

C.5.1.6 SUBTASK 1.6 – UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The PMP is an evolutionary document that shall be updated annually at a minimum (Section F, Deliverable 10). The contractor shall work from the latest Government-approved version of the PMP.

C.5.1.7 SUBTASK 1.7 – PREPARE TRIP REPORTS

The Government will identify the need for a trip report when the request for travel is submitted (Section F, Deliverable 11). The contractor shall keep a summary of all long-distance travel including, but is not limited to, the name of the employee, location of travel, duration of trip, and Point of Contact (POC) at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any

SECTION J - ATTACHMENTS

knowledge gained. At a minimum, trip reports shall be prepared with the information provided in Section J, Attachment G.

C.5.1.8 SUBTASK 1.8 – UPDATE BASELINE QUALITY CONTROL PLAN (QCP)

The contractor shall update the QCP submitted with its proposal (Section F, Deliverable 12) and then provide a final baseline QCP as required in Section F (Section F, Deliverable 13). The contractor shall periodically update the QCP, as required in Section F (Section F, Deliverable 14), as changes in program processes are identified.

Within the QCP, the contractor shall identify its approach for providing quality control in meeting the requirements of the TO. The contractor's QCP shall describe its quality control methodology for accomplishing TO performance expectations and objectives. The contractor shall fully discuss its validated processes and procedures that provide high quality performance for each Task Area. The QCP shall describe how the processes integrate with the Government's requirements.

C.5.1.9 SUBTASK 1.9 – SECURITY EDUCATION

The contractor shall provide a Security Education Plan (Section F, Deliverable 20). The plan shall identify activities that will ensure all contractor personnel assigned to the program fully understand the sponsor's security requirements, any requirements specific to the business areas serviced under this acquisition, and the consequences of non-compliance. The plan shall also include, but is not be limited to, providing continuing security awareness; debriefing personnel departing the program in a timely manner; ensuring the proper handling of classified data, program-specific data, and Government information; ensuring proper control and classification of program documentation and data; and identifying a process for providing timely notification of security-related issues to the Contracting Officer's Security Representatives (COSR) and an email confirming delivery to the COSR to the FEDSIM COR, to include a feedback loop for corrective actions taken.

C.5.2 TASK 2 – PROVIDE TRANSITION SUPPORT

The contractor transition support shall include having all tasks staffed with fully qualified personnel, having a plan to integrate staff and assure staff is fully trained, taking over services with no degradation to services, assuming full responsibility for management of all TO requirements, as well as having a plan to transition and deliver all material and information to the Government at the end of the TO.

C.5.2.1 SUBTASK 2.1 – TRANSITION-IN

The contractor shall update the draft Transition-In Plan (Section F, Deliverable 15) provided with its proposal and provide a final Transition-In Plan as required in Section F (Section F, Deliverable 16). The Government will make all classified information available to complete Transition-In at Project Start (PS). The Government will complete in-person training to expedite the required information and data system access training. The contractor shall provide standard Form 4311 (Section J, Attachment I) for each of the contractor's priority staff and all priority staff shall be included on the Contractor Personnel Security Summary List (Section J, Attachment AF) at Task Order Award (TOA). The contractor's priority staff shall include all cleared personnel that the contractor deems are required to complete the proposed Transition-in

SECTION J - ATTACHMENTS

plan and continue operations post Transition-in. O&M personnel are a top priority for successful transition-in and all O&M staff must have an ODNI Industrial Security Staff-Like Approval/Top Secret (ISSA/TS) with Full Scope Polygraph security clearance prior to getting approval to start work and shall be included as part of the contractor's priority staff. The contractor shall ensure that there will be minimal disruption and degradation to vital Government business and zero disruption and degradation after transition-in is completed. The contractor shall implement its Transition-In Plan at PS, and all transition activities shall be completed 120 days after approval of the final Transition-In Plan (Section F, Deliverable 16). The contractor's Transition-In Plan shall include the transition of the NCTC Portfolios detailed in the Draft Systems Technical Roadmap (Section J, Attachment X).

C.5.2.2 SUBTASK 2.2 – TRANSITION-OUT

The contractor shall provide Transition-Out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a draft Transition-Out Plan within six months after PS (Section F, Deliverable 17). The Government will work with the contractor to finalize the Transition-Out Plan (Section F, Deliverable 18) in accordance with Section E. At a minimum, the Transition-Out Plan shall be reviewed and updated on an annual basis (Section F, Deliverable 19). Additionally, the Transition-Out Plan shall be reviewed and updated quarterly during the final Option Period (Section F, Deliverable 19).

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

- a. Project management processes.
- b. POCs.
- c. Location of technical and project management documentation.
- d. Status of ongoing technical initiatives.
- e. Appropriate contractor to contractor coordination to ensure a seamless transition.
- f. Transition of Key Personnel.
- g. Schedules and milestones.
- h. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

The contractor shall implement its Transition-Out Plan NLT six months prior to expiration of the TO.

C.5.3 TASK 3 – DEVELOPMENT SUPPORT

The contractor development support shall include Architecture Support, System Engineering, Software Engineering Development and Integration, Algorithm Development, Security planning and compliance (including achieving ATO), System Level Testing, and innovation development and implementation including but is not limited to:

SECTION J - ATTACHMENTS

- a. Standing up a development, integration, and test environment with a process for rapid development and enterprise-wide implementation, when necessary.
- b. Enabling the ability to integrate and test Commercial Off-The-Shelf (COTS)/Government Off-The-Shelf (GOTS) products (as an entire solution or as part of an overall system solution).
- c. Enabling the ability to quickly augment and enhance existing tools, applications, and methodologies to advance analytic efforts and maintain currency with changing terrorism milieu.
- d. Developing the necessary Transition Planning including user training, support staff training, and any applicable decommissioning activities for systems/services that have been replaced.

The contractor shall implement a system/software lifecycle management process, in coordination with the Government, to achieve a single lifecycle for the program that includes planning, designing, developing, integrating, and testing verification and validation activities applicable to both enhancement of current technologies and creation of new capabilities; that includes, but is not limited to, automation, data science, big data analytics, data ingestion and manipulation, machine learning, emerging technologies, social media exploitation, social network analysis, alerting and warning, and advancing traditional analytic methods.

The contractor shall identify and apply modern development best practices, including DevOps and Agile development practices that provide for the rapid development and automated fielding of capabilities, and the establishment of a continuous integration, delivery, and user feedback methodology resulting in systematic, repeatable, secure, and streamlined delivery of capabilities to the production environments.

The contractor shall provide comprehensive documentation and information necessary to monitor the DevOps processes, procedures, and/or policies that were implemented in the creation of the applications.

C.5.3.1 SUBTASK 3.1 – APPLIED TECHNOLOGY ENHANCEMENTS TO BASELINE SYSTEMS, SOFTWARE, AND SERVICES

The contractor shall support the continued enhancement of systems, software, and tools that are in a hybrid lifecycle phase (development and operations). These enhancements are coordinated with the NCTC users through the appropriate governance forum to gather and prioritize their needs.

The contractor shall provide applied technology enhancements to baseline systems, software, and services which include, but are not limited to, the following:

- a. Developing enhancements for new and improved user functionality with quick turnaround for those systems that the contractor has software and operations responsibilities.
- b. Performing analysis and recommending enhancements to extend the life or improve reliability of the equipment when critical equipment is no longer supportable by repair or replacement.

SECTION J - ATTACHMENTS

- c. Developing capability enhancements in response to National Security events that are unplanned and unknown in advance, as well as rapid adjustments/enhancements to address the changing terrorism milieu.
- d. Identifying and implementing products and techniques to automate the capability delivery process to operations, as well as automating the feedback loops from mission operations and obtaining timely feedback from mission operations during the development process.

C.5.3.2 SUBTASK 3.2 – REQUIREMENTS MANAGEMENT

The contractor shall support the requirements management process of documenting, analyzing, tracing, prioritizing, and agreeing on requirements and then controlling changes and communicating with relevant stakeholders.

The contractor shall provide requirements management services which include, but are not limited to, the following:

- a. Identifying, collecting, assessing, and decomposing CT service, application, and tool requirements into product and product component (system technical) requirements and derived requirements that support design and development activities.
- b. Establishing a means to control and track changes to requirements.
- c. Managing the requirements baseline allocated to projects including any approved changes.
- d. Maintaining bi-directional traceability by establishing and maintaining the Requirements Verification Traceability Matrix (RVTM) (Section F, Deliverable 24); mapping the enterprise requirements baseline to the system/functional baseline and ultimately to the build baseline through system verification activities.
- e. Providing the capability for stakeholders to routinely obtain status of open and closed requirements.
- f. Documenting and managing user stories to support development priorities when using the Agile development model.
- g. Creating and updating individual product backlogs resulting from an Agile development approach.

C.5.3.3 SUBTASK 3.3 – SYSTEMS ENGINEERING

The contractor shall provide systems engineering, covering the lifecycle of IT projects and services, to include application and services development, O&M, and cloud and infrastructure design and implementation.

The contractor shall provide systems engineering services to include, but is not limited to:

- a. Supporting the Government in the use of systems engineering processes and standards established by the Government sponsor and recognized systems engineering accrediting organizations.
- b. Conducting analyses and trade studies including the identification and evaluation of COTS and GOTS capability required to identify capability gaps, IT solutions, and technology integration opportunities.

SECTION J - ATTACHMENTS

- c. Developing and updating system CONOPS documents outlining the significant aspects of a proposed solution as required.
- d. Performing structured requirements analysis to decompose high-level needs into functional, product, and product component (system technical) requirements and derived requirements that support design and development activities.
- e. Ensuring requirements are complete, unambiguous, documented, actionable, measurable, testable, traceable to a need, and defined to a level of detail sufficient for system design.
- f. Assisting in the design and development of new and/or modified system solutions that:
 - 1. Incorporate software, data, network, and/or hardware requirements to meet mission requirements and improve operational efficiency of customers.
 - 2. Consider the current and target NCTC IT architectures, the NCTC Products Baseline, and products recommended from the Technology Insertion Program.
 - 3. Are sufficiently detailed to generate a Rough Order of Magnitude (ROM) to implement the solution.
 - 4. Implement automated approaches to enable continuous capability enhancements and a robust feedback loop to users.
 - 5. Enable rapid ingestion/Extract, Transform, and Load (ETL) of ad hoc datasets for rapid analytic access.
- g. Assisting in the delivery of system and infrastructure capabilities that scale to meet enterprise demand with the least re-engineering effort possible.
- h. Identifying requirements for extensibility and scalability to increase capacity to a level appropriate with the use, anticipated loading, and mission criticality; to decrease capacity for unused and excess capacity; and for sustainability, Continuity of Operations (COOP), backup, and recovery services necessary to support established Service Level Agreements (SLAs).
- i. Developing, delivering, and maintaining a system inventory which provides a mapping of system requirements to hardware elements and software elements that are required by the resulting system.
- j. Participating and supporting the development of implementation strategies and courses of action that address mission capabilities innovation, development and implementation, data ingestion and migration, and capacity planning.
- k. Facilitating and monitoring the integration, interoperability, and synchronization of enterprise-wide data, systems, and infrastructure solutions and services.

C.5.3.4 SUBTASK 3.4 – HARDWARE DESIGN AND INSTALLATION

The contractor shall provide hardware design and installation services which include, but are not limited to, the following:

- a. Completing the detailed design of the Hardware Configuration Items (HWCIs) that comprise the systems.
- b. Defining the hardware components required to update the development, test, and production environments and to support a DR capability.
- c. Preparing procurement packages to deliver the required hardware.

SECTION J - ATTACHMENTS

- d. Building, installing, and configuring hardware to support development and test activities, upon receipt of the development and test hardware.
- e. Developing hardware build and installation procedures that provide instructions on building and installing the hardware in the production and DR environments.
- f. Building and installing the procured hardware at production sites using the hardware build and installation procedures.

C.5.3.5 SUBTASK 3.5 – SOFTWARE ENGINEERING, DEVELOPMENT, AND INTEGRATION

The contractor shall provide software engineering, development, and integration services which include, but are not limited to, the following:

- a. Applying current industrial software development and DevOps best practices that include rapid, iterative, and incremental project management techniques and Agile software development.
- b. Developing documents and/or deliverables that define the requirements baseline and the deployment of capabilities to operations.
- c. Completing the design, development, integration, test, and deployment of all software including explicit feedback loop processes between operations, test, and development activities. This capability includes software for mission algorithms, applications and tools, web and portal systems, and/or knowledge and content management capability.
- d. Accounting for the identification of feedback opportunities (from testing, operations, end-users, etc.) in software engineering, development, and integration. Furthermore, once identified, such feedback loops shall be regularly examined, refined, and made more robust.
- e. Enhancing software functionality based on rapidly evolving mission needs and technology opportunities.
- f. Delivering and documenting all software source code (COTS, GOTS, and custom) and providing version description documentation that defines the software modules, configuration files, and scripts, by version number, required for the production system. This document shall also provide a list of defects that were known to exist in the software at time of delivery.
- g. Updating the system inventory with the list of software components that will be loaded and executed on the various HWCIs within the production system.
- h. Documenting the tools and processes used to build and install the software in the production environment.
- i. For Cloud development and legacy migration, the contractor shall be responsible for the following:
 - 1. Providing cloud service expertise to include developing applications to run on a cloud infrastructure in accordance with Government defined standards and within Government defined frameworks.
 - 2. Migrating and enhancing mission algorithms, applications, and tools for the cloud, as directed by the Government.

SECTION J - ATTACHMENTS

C.5.3.5.1 SUBTASK 3.5.1 – AGILE SOFTWARE DEVELOPMENT

The contractor shall use Agile methodologies for software development, where the development is organized into one or more releases consisting of multiple sprints. The frequencies and durations of the releases and sprints shall be defined during project planning. The contractor shall provide weekly progress updates, and demonstrations, as required, to the government and shall update the contractor schedule for the WSR (Section F, Deliverable 27).

During project planning, the project defines team structure, development environment, system requirements, mission interaction; and, the contractor shall review the architectural specification, high level system design, and current supporting processes. The contractor shall deliver a Development Sprint Plan (Section F, Deliverable 28) to document the design approach, Agile code development, integration, test, quality, and configuration control processes and procedures that will be utilized in the project, involving mission elements to verify design, functionality, and implementation plans.

The contractor shall coordinate with Government, as required, during project preparation or development sprints for the performance of the following tasks including, but is not limited to:

- a. Identifying and setting up all necessary tools to support the development and management activities.
- b. Identifying processes and plans for mission interaction to understand mission needs, gather requirements, validate design and planning implementation, acquire feedback, and deliver products and capabilities commensurate with mission needs and priorities.
- c. Establishing the most effective Agile framework
- d. Defining processes such as code control, daily builds, regression tests, etc.
- e. Defining or updating processes and procedures for configuration control.
- f. Coordinating with Security and preparing or updating security-related documentation.
- g. Setting up and testing the Integrated Development Environment and other development tools.
- h. Defining processes for documenting user stories, business priorities, and planned enhancements with the estimated effort for each requirement.
- i. Producing or updating the Interface Control Document and Interface Design Document(s) to identify and characterize all the external interfaces.
- j. Producing or updating the System Design Document (SDD) (Section F, Deliverable 31) including System Architecture Design and the design of external interfaces to be extensible and scalable.
- k. Producing or updating the Database Design Document (DBDD) (Section F, Deliverable 32) documenting the logical database schema.
- l. Producing or updating the Test and Evaluation Master Plan (TEMP) (Section F, Deliverable 33).
- m. Identifying the list of software tools, licenses and hardware needed by the team for development and documentation in the Bill of Materials (BOM).
- n. Producing or updating User Training Plan (Section F, Deliverable 35).

The contractor shall develop a Release Plan (Section F, Deliverable 29), based on backlog priorities set by the Government and aligned with a product roadmap that documents the schedule and contents of proposed system releases for deployment. The contractor shall coordinate with the Government and update the release plan prior to each release deployment.

SECTION J - ATTACHMENTS

The contractor shall coordinate with the Government and conduct a Sprint Planning meeting to plan each sprint based on backlog priorities, estimated effort required, and the scope and resources available during the sprint. The contractor shall document the planned requirements for the Sprint in the Sprint Backlog.

In conducting Agile sprints, the contractor shall complete tasks which include, but are not limited to, the following:

- a. Designing and coding the system to meet the requirements documented in the Sprint Backlog.
- b. Demonstrating each sprint release to the Government and mission owner for approval to deploy to the testing environment.
- c. Developing the system and interface test procedures, test cases and test data in accordance with the TEMP. The test procedures shall include, but are not limited to, test pre-conditions, test sequences, and anticipated results/assertions.
- d. Updating RVTM (Section F, Deliverable 22)
- e. Performing functional tests and documenting the test results. The functional tests shall address the verification that all requirements, specified in the Sprint Backlog, have been met.
- f. Conducting a sprint review/retrospective on the final day of the sprint to include final accounting of user stories planned, completed, added, and deferred with demonstrations of functionality completed during the sprint.

The contractor shall conduct a sprint review to update and re-prioritize a product backlog as appropriate. The Sprint Review shall include reviewing technical details of features developed in the Sprint, documenting lessons learned, documenting development metrics, and updating a product backlog, as required. A summary of the results of the sprint review, identifying the technical accomplishments of the sprint cycle, shall be documented in a Sprint Summary Report (Section F, Deliverable 30) and described in non-technical terms. The Sprint Summary Report shall include user stories, planned, completed, added, and deferred.

C.5.3.6 SUBTASK 3.6 – APPLICATION/SECURITY ENGINEERING

The contractor shall support application security activities related to the configuration and implementation of software applications and their related infrastructure to satisfy identified security procedures and policies.

The contractor shall provide application/security engineering services which include, but are not limited to, the following:

- a. Executing system security processes and controls as defined in Intelligence Community Directive (ICD) 503, IC Information System (IS) Risk Management, Certification and Accreditation and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 1, Applying the Risk Management Framework (RMF) to Information Systems Security, and further elaborated in additional Committee on National Security System Instructions (CNSSI) 1253 with the objective of obtaining an ATO.
- b. Following the guidelines of the ODNI ICD 503 process and the Body of Evidence (BOE) (Section F, Deliverable 36) to prescribe common controls as defined by the Agency on

SECTION J - ATTACHMENTS

whose network the system resides. The BOE shall be an agreed upon collection of artifacts that the contractor shall produce, either in whole or in part, enabling the Authorizing Official to make risk-based decisions regarding the use of the system.

- c. Reviewing and updating system security plans and privileged and general user's guides. Depending on whether the effort is new or ongoing, the additional information that may be required within the BOE includes:
 - 1. CONOPS.
 - 2. All approved Memorandums of Understanding (MOUs), Memorandums of Agreement (MOAs), Interconnectivity Agreements, and Production Data Waivers (PDWs).
 - 3. System Control Traceability Matrix (SCTM).
 - 4. Plan of Action and Milestones (POA&M).
 - 5. Scan Results (internal).
 - 6. Scan Results (from the Security Control Assessor).
 - 7. Security Assessment Report.
 - 8. Risk Assessment Report.
 - 9. Continuous Monitoring Plan.
- d. Delivering the agreed to BOE and all letters of adjudications/dispositions, interim or full.

C.5.3.7 SUBTASK 3.7 – SYSTEMS INTEGRATION

The contractor shall provide systems integration services which include, but are not limited to, the following:

- a. Identifying component subsystems of the overall system and determining the requirements for ensuring that the subsystems work together to function as a single system, including integration paths for partner agency data, both regularly shared and ad-hoc in nature, to enable rapid exposure to analysts.
- b. Planning, documenting, and maintaining solutions to total systems or subsystems that use internally created and/or COTS products.
- c. Providing a total system perspective to include relationships, dependencies, and requirements of hardware and software components.
- d. Researching COTS and GOTS solutions to solve integration problems and/or meet system requirements.
- e. Ensuring that the mission applications/tools, web systems, and portals integrate effectively with existing enterprise systems and data stores with the goal of maintaining a well-connected, secured, and controlled enterprise of systems that maintains high systems availability with rapid development and exposure to analysts.
- f. Ensuring services development follow the structured development, test, and release management processes in addition to stringent change management and configuration control and enforcement of SLAs. Identifying, developing, coordinating, maintaining, delivering, and updating required interface specifications. Including the definition of services, data flows, and dependencies for internal and external service providers.

SECTION J - ATTACHMENTS

- g. Integrating and optimizing workflow, automation, manual processes (where necessary), and feedback loops across the DevOps environment and with mission owner elements to enable automated, continuous capability delivery to mission.

C.5.3.8 SUBTASK 3.8 – COMMERCIAL-OFF-THE-SHELF (COTS)/DEVELOPED APPLICATIONS INTEGRATION

The contractor shall integrate approved COTS products and perform integration services including, but is not limited to, the following:

- a. Performing COTS/developed applications system engineering, baseline integration, deployment package creation, functional acceptance/compatibility testing, and supporting the deployment of Government sponsor directed solutions to ensure successful incorporation into the operational baseline (new or upgrades).
- b. Integrating approved COTS/developed applications upgrades into the baseline.
- c. Providing support for resolution of DRs in integrated COTS software.
- d. Engineering, developing, integrating, and maintaining software code as necessary to integrate COTS/developed applications information solutions to deliver requested capabilities, based on mission needs and approved requirements.

C.5.3.9 SUBTASK 3.9 – SYSTEM AND DATA MIGRATION

The contractor shall provide system and data migration services which include, but are not limited to, the following:

- a. Preparing and documenting plans for migrating data, personnel, and system operation from the existing, legacy systems to a new environment (e.g., new system, Commercial Cloud Services (C2S), etc.).
- b. Preparing migration procedures that describe the steps and activities required to complete migration from the legacy system to the new environment.
- c. Developing back-out procedures required to return the enterprise to a legacy operational state, in the event that a difficulty is encountered in one or more steps during the migration.

C.5.3.10 SUBTASK 3.10 – SYSTEM TESTING

As part of the development process, the contractor shall complete testing, in accordance with a Government-approved governance process which include, but are not limited to, the following:

- a. Establishing evaluation criteria and conducting evaluations for system capability verification and validation.
- b. Implementing a centrally managed test process.
- c. Documenting testing requirements for evolving system capabilities.
- d. Identifying the test verification and validation environment.
- e. Establishing automated testing in keeping with continuous delivery models to include developer, unit, integration, component, and qualification testing.
- f. Developing, maintaining, delivering, and executing test plans and procedures that verify and validate incremental capability delivery.

SECTION J - ATTACHMENTS

- g. Providing documentation and analysis of test verification results.
- h. Working with mission owner elements and users to ensure that user requirements and issues are addressed by the test processes prior to deployment.
- i. Participating in mission application acceptance/validation testing, including back-out plans for any changes to the existing baseline, as approved by the governance process.
- j. Establishing an approach to reuse documented test processes, plans, and procedures on various mission applications.
- k. Documenting user feedback for incorporation into future development activities.

C.5.3.11 SUBTASK 3.11 – DEVELOPMENT, INTEGRATION AND TEST ENVIRONMENT

The contractor shall support a development and test environment which include, but are not limited to, the following activities:

- a. Implementing and maintaining an environment necessary to support the design, development, integration, and testing (verification and validation) of applications, tools, and web and portal services prior to promoting into the operational baseline.
- b. Including a staging environment as well as an explicit connection to the operational environment(s).

C.5.4 TASK 4 – SYSTEMS O&M SUPPORT

The contractor shall provide systems O&M support, troubleshooting, and repair of supported systems. The contractor shall analyze test data and report the results in an O&M Status Report (Section F, Deliverable 25).

The contractor shall provide system and software O&M support which include, but are not limited to, the following:

- a. Identifying all recurring system and software O&M activities including maintaining and enhancing interfaces to and from COTS software.
- b. Documenting all operations performed by end users, system operators, and system maintainers including periodic, scheduled maintenance.
- c. Providing corrective, adaptive, perfective, and preventive maintenance. The contractor shall support the Government's current maintenance processes and adapt new processes, as appropriate. Current processes include:
 - 1. Corrective maintenance: Reactive modification of a software product performed after delivery to correct discovered problems.
 - 2. Adaptive maintenance: Modification of a software product performed after delivery to keep a software product usable in a changed or changing environment (i.e., adding new drop down menus, linking application to new data, and adding queries to applications to further utilize inherent algorithms).
 - 3. Perfective maintenance: Modification of a software product after delivery to improve performance or maintainability.
 - 4. Preventive maintenance: Modification of a software product after delivery to detect and correct latent faults in the software product before they become effective faults.

SECTION J - ATTACHMENTS

- d. Documenting all hardware and software maintenance support actions and licenses required to successfully provide O&M support to the system.
- e. Delivering all source code, scripts, documentation, and datasets that have been modified in support of system and software maintenance.
- f. Supporting the Government in preparing operational readiness plans that will be executed with mission counterparts to demonstrate and validate system operations in a production/operational environment.
- g. Supporting the Government during operational readiness reviews.
- h. Providing O&M support during the Government operational demonstration periods including:
 - 1. Providing training to new operators while also conducting “Train-the-Trainer” training.
 - 2. Monitoring system performance and user operations to detect and/or analyze anomalies that may occur once the system is deployed and used in its operational environment.
 - 3. Developing enhancements to the deployed software capability for an identified period after the initial deployment.
- i. Supporting the Government in preparing operational readiness reports that document the results obtained during operational demonstration periods.
- j. Providing support to the Government during operational acceptance reviews to obtain mission acceptance of the delivered capability.

C.5.4.1 SUBTASK 4.1 – NCTC SERVICES SUPPORT

The contractor shall provide the NCTC services support which include, but are not limited to, the following:

- a. Service Operational Specifications shall include, but is not limited to, developing, delivering, and maintaining Service Operational Specifications for the identified NCTC services. Service Operational Specifications define the minimum salient characteristics necessary for all end user hardware (e.g., minimum hardware specifications and configuration parameters for processor speed, memory, storage, ports, device software, monitor resolution) in order to support operation of the delivered services. Service Operational Specifications also define the salient characteristics necessary for operational hosting of the NCTC services.
- b. Service Level Management shall include, but is not limited to, the following:
 - 1. Recommending service level requirements.
 - 2. Monitoring and reporting on the actual service level (service level reporting).
 - 3. Planning and implementing continuous improvements in service levels.
 - 4. Coordinating service management and service support functions.
 - 5. Conducting service review meetings with customers.
 - 6. Implementing service improvement programs.
 - 7. Monitoring the changing requirements, amendments to SLAs, operation level agreements, and other support agreements with external suppliers.
 - 8. Preparing and maintaining a service catalog.

SECTION J - ATTACHMENTS

- c. Service Delivery shall include, but is not limited to, the following:
 - 1. Determining usage specifications.
 - 2. Transposing the requirements to system utilization specifications.
 - 3. Determining the required resources.
 - 4. Preparing and maintaining a capacity plan.
 - 5. Monitoring the performance and performing fine-tuning.
 - 6. Performing improvements to achieve the agreed service level and usage specifications.
- d. Service Availability Management shall include, but is not limited to, the following:
 - 1. Determining availability specifications.
 - 2. Preparing availability forecasts and planning the required measures.
 - 3. Preparing an availability plan.
 - 4. Determining the actual availability.
 - 5. Preparing reports.
 - 6. Improving the agreed availability.
- e. Service Continuity Management shall include but is not limited to, the following:
 - 1. Performing risk analyses as part of continuity management.
 - 2. Preparing recovery plans for IT services.
 - 3. Providing the required means.
 - 4. Providing user training.
 - 5. Testing and verifying plans to be able to restore the services in an emergency in the time required, safely, and in a controlled way.
 - 6. Keeping recovery plans up to date.
- f. Data Backup, DR, and COOP shall include, but is not limited to, the following:
 - 1. Providing support for planning, executing, and managing Enterprise data backup, DR, and COOP operations and support.
 - 2. Ensuring Enterprise data backup, DR, and COOP requirements are considered early in the application or systems' development lifecycle.
 - 3. Verifying Enterprise data backup, DR, and COOP capabilities during installation.
 - 4. Creating and executing recurring Enterprise data backup, DR, and COOP scenarios to test and verify continued capabilities.

C.5.4.2 SUBTASK 4.2 – SYSTEM AND USER SUPPORT

The contractor shall provide system and user support which include, but are not limited to, the following:

- a. Outreach and Relationship Management to Support Agile and DevOps Environments shall include, but is not limited to, the following:
 - 1. Developing, maintaining, delivering, and executing a comprehensive plan for customer outreach and Customer Relationship Management (CRM).
 - 2. Defining the plans, processes, and methods for managing coordination and communications with the stakeholder community.

SECTION J - ATTACHMENTS

3. Supporting both broad and targeted stakeholder coordination and communications of relevant activities, schedules, testing, and service capabilities, to increase awareness customer confidence, and to improve customer satisfaction levels.
 4. Developing the plans, processes, tools, and techniques to collect user feedback and customer satisfaction (e.g., surveys, questionnaires); analyze and assess results; identify and recommend opportunities for continuous improvement; and report results and recommendations back to the Government.
- b. Mission Engagement and Operations Planning shall include, but is not limited to, the following:
1. Supporting the critical linkage between customer mission planning and IT support planning to include understanding mission operations and needs, mission owner element testing prior to deployment, and user feedback mechanisms.
 2. Exercising support planning.
 3. Analyzing operational performance measurements and associated trends to ensure services meet customer missions, goals, and objectives.
- c. Access Management shall include, but is not limited to, the following:
1. Recommending and implementing an Access Management process that establishes processes and creates and maintains user accounts for mission applications.
 2. Establishing, processing, creating, and maintaining user accounts for prototype and developmental systems.
- d. Event Management shall include, but is not limited, to the following:
1. Recommending and implementing an Event Monitoring process that monitors system breaches and logs and tracks events for applications and services.
 2. Escalating events, when applicable, to incidents or problems and recording when they are addressed and closed.
 3. Monitoring the network and supporting infrastructure for breaches, logs, and tracking events.
- e. Request Fulfillment shall include, but is not limited to, the following:
1. Recommending and implementing a Request Fulfillment process that responds to user requests in a timely manner.
 2. Maintaining operational level configuration items to include, but is not limited to, application documentation, training materials, system design documentation, and/or application operation start up/power down procedures.
- f. Service Desk shall include, but is not limited to, the following:
1. Providing a strategy for developing and resourcing a Service Desk (virtual federated or physical) to act as a central POC between the customer and the NCTC to resolve customer issues at the lowest practical support level and provide a consistent and quality customer experience across enterprise service areas.
 2. Using of a common Information Technology Service Management (ITSM) tool set to document, process, and monitor incidents, problems, inquiries, and change and service requests, as well as coordinate new capabilities through an actionable service catalog and support for other IT service management functions.
- g. Tier Support shall include, but is not limited to, the following:

SECTION J - ATTACHMENTS

1. Tier 1 Support (e.g., Accounts for Applications) - This is the initial support level responsible for basic customer issues.
 2. Tier 2 Support (e.g., Process Restart, Simple SOPs, No Code Changes, and Triage to Tier 3) - This is more in-depth technical support level than Tier 1 as the technicians are more experienced and knowledgeable on a particular product, service, or technology.
 3. Tier 3 Support (e.g., Debug, Code Fix) - Tier 3 specialists are responsible for handling the most difficult or advanced problems.
- h. Desk-Side Support shall include, but is not limited to, the following:
1. Providing deskside assistance to resolve customer incidents and locally resolving systems account and access management issues.
 2. Tailoring directory service entries, organizational mailboxes, and distribution lists to meet customer requirements.
 3. Loading approved add-on applications to the workstation baselines.
 4. Supporting equipment install, move, add, change requests; and configuring, troubleshooting, and maintaining end-user devices and peripherals.
- i. Incident Management shall include, but is not limited to, the following:
1. Recommending and implementing an Incident Management process.
 2. Providing initial incident analysis and initiating initial support.
 3. Handing off to additional support if the fault cannot otherwise be fixed.
 4. Increasing the resources if there is a danger of failing to meet the agreed service levels.
 5. Fixing the fault and restoring the service.
 6. Evaluating incidents and preparing reports on service improvements.
- j. Problem Management shall include, but is not limited to, the following:
1. Providing a process that accounts for reactive, proactive, and preventative activities.
 2. Recommending and implementing a problem management process.
 3. Providing 24x7 Problem Management including:
 - i. Problem handling.
 - ii. Error handling.
 - iii. Incident support.
 - iv. Proactive problem management that includes measures of error prevention, trend analyses, actions and measures, and preparation of quality reports.

C.5.4.3 SUBTASK 4.3 – CONFIGURATION MANAGEMENT (CM) SUPPORT

The contractor shall support CM services to maintain technical and administrative control of the functional and physical characteristics of technology assets and provide continuous visibility into the types and numbers of assets throughout the enterprise. The contractor shall provide CM support which include, but are not limited to, the following:

- a. Change Management:

SECTION J - ATTACHMENTS

1. Receiving and recording Requests for Changes (RFCs) (Section F, Deliverable 26).
 2. Submitting RFCs to the Government for inclusion in the appropriate governance process for adjudication.
 3. Assessing the ramifications, costs, benefits, and risks of the planned changes.
 4. Updating the change/release plan.
 5. Coordinating and controlling change implementation.
 6. Monitoring and reporting on the success of implementation.
 7. Updating the CM database.
 8. Updating relevant development plans and architectures.
 9. Completing and reviewing the RFCs (post-implementation review).
- b. NCTC mission IT Services Training
1. Developing, maintaining, delivering, and executing a comprehensive approach and methods for training to support effective use and O&M of the NCTC mission IT services.
 2. Preparing training plans, training curricula, materials, and schedules.
 3. Performing training.
 4. Evaluating training success.
 5. Defining, documenting, maintaining, and delivering SOPs and knowledge base modules that provide users with instructions that support and encourage “self-help” and “self-training.”

C.5.4.4 SUBTASK 4.4 – RELEASE AND DEVELOPMENT SUPPORT

The contractor shall provide release and development support which include, but are not limited to, the following:

- a. Providing release planning details for when service requirements and capabilities will be available.
- b. Providing plans and processes for implementation, testing, independent verification, assessments and authorization, deployment, and acceptance of services into the operational environment.
 1. Providing details for employing continuous delivery/deployment practices and/or mechanisms.
 2. Changing or developing any deployment scripts.
 3. Testing the deployment plan and scripts as part of the production-ready test.
 4. Validating the production-ready test outcome by unit testing and/or independent verification and validation (IV&V) and approved for production via the approved governance process.
- c. Working with the Government to release, distribute, and install new and upgraded software.
- d. Working with the Government to install new or modified hardware.
- e. Providing plans and processes for establishing and maintaining configuration and quality control of all the NCTC services, software, middleware, and hardware assets.

SECTION J - ATTACHMENTS

- f. Providing information and training prior to delivery.
- g. Storing the released software (source code, scripts, documentation, datasets, etc.) in a definitive software library, as identified by the Government in accordance to DevOps methodology.

C.5.4.5 SUBTASK 4.5 – SOFTWARE AND HARDWARE MANAGEMENT AND CONTROL

The contractor shall provide software and hardware management and control which include, but are not limited to, the following:

- a. Identifying requirements for software, software licenses, and maintenance agreements to support CT Service functionality where software licenses cannot be provided as Government-Furnished Property (GFP).
- b. Identifying requirements for hardware and associated maintenance for server based hardware requirements and other non-end user device equipment.
- c. Identifying requirements for hardware and software to support innovation, development, integration, and test environments.
- d. Developing, delivering, maintaining, and implementing plans, processes, and techniques to identify, quantify, and monitor hardware and software assets (including licenses and maintenance agreements).
- e. Providing the capabilities necessary to define, track, and control licenses procured under the contract and those licenses provided by the Government for the full period of performance of the contract. This capability should be on-line/remotely accessible through standard features (e.g., browser) to provide Government with situational awareness and ensure compliance with applicable license terms and conditions.
- f. Delivering Hardware/Software Reports (Section F, Deliverable 21) to track/audit hardware (equipment, parts, and materials) and software vendors, titles, licenses, quantities, costs, versions, and usage to ensure compliance with the terms and conditions of each.
- g. Maintaining records in accordance with Government identified policies to support audit requirements.

C.5.4.6 SUBTASK 4.6 – SERVER ADMINISTRATION AND MANAGEMENT

The contractor shall provide server administration and management which include, but are not limited to, the following:

- a. Providing server administration and management for virtual and physical servers. Services include building, documenting, operating, maintaining, and sustaining enterprise, regional, and local physical and virtual servers supporting mission applications and systems as well as the underlying shared application and infrastructure services.
- b. Installing, configuring, and maintaining servers or other computer systems.
- c. Documenting computer hardware, system support, diagnostic software, and configuration settings for the full lifecycle of the delivered capability.
- d. Planning for and responding to service outages and other problems.

SECTION J - ATTACHMENTS

- e. Installing system upgrades.
- f. Managing system resources and optimizing system performance.
- g. Performing system startup, shutdown, diagnostics, file management, user and group setups, and determination of login scripts.
- h. Assisting in the coordination of system downtime planned for maintenance, system patches, upgrades, or new releases.
- i. Performing data and file storage administration and related functions including provisioning and monitoring backups and restorations.
- j. Ensuring computer operators are properly trained.
- k. Consulting on computer problems beyond the knowledge of the customer and technical support staff.
- l. Providing support for Microsoft (MS), LINUX, and Unix-based COTS server environments, and other operating systems on a case by case basis.

C.5.4.7 SUBTASK 4.7 – STORAGE ADMINISTRATION AND MANAGEMENT

The contractor shall provide storage administration and management which include, but are not limited to, the following:

- a. Supporting the provisioning of storage services across all virtual and physical environments including administration, management support, backup, DR, and COOP.
- b. Monitoring, allocating, and recommending system storage usage in accordance with appropriate directives.
- c. Documenting all instances of storage within the enterprise and storage services capabilities to include size, speed, accessibility, and scalability.
- d. Applying, maintaining, and troubleshooting storage-related issues.
- e. Providing data protection and management solutions, scalable from workgroup to enterprise, and ensure COOP and efficient use of storage across the enterprise. This includes both the management of storage as well as back-up and recovery functions.
- f. Operating server and storage appliances.
- g. Analyzing and resolving common problems related to servers and storage.
- h. Installing patches and performing system updates.
- i. Managing server and storage processing strategies.
- j. Recovering data.
- k. Installing and configuring server and storage devices.

C.5.4.8 SUBTASK 4.8 – NCTC SERVICES, ADMINISTRATION, AND MANAGEMENT

The contractor shall provide NCTC services, administration, and management which include, but are not limited to, the following:

- a. Providing mission system services, administration, and management support for both traditional systems and systems that exist within or use virtual and cloud services hosted by other agencies and external cloud service providers.

SECTION J - ATTACHMENTS

- b. Services that include specialized systems, database, and other functions tailored for enterprise, regional, and/or specific mission applications and systems.

C.5.4.9 SUBTASK 4.9 – SHARED APPLICATION AND INFRASTRUCTURE SERVICES, ADMINISTRATION, AND MANAGEMENT

The contractor shall provide shared application and infrastructure services, administration, and management which include, but are not limited to, the following:

- a. Providing Cloud Platform as a Service (PaaS) capabilities.
- b. Providing support to integrate native cloud infrastructure with C2S and IC Cloud Infrastructure as a Service (IaaS) capabilities, and delivering and managing Government-specific IaaS to the users to provision processing, storage, networks, and other fundamental computing resources where the user is able to deploy and run mission specific software, including operating systems and applications. These services shall include, but are not limited to, systems database and account administration to operate, maintain, and sustain the enterprise shared applications and infrastructure services.
- c. Managing and controlling cloud infrastructure including network, servers, operating systems, storage, and platform software and services.

C.5.4.10 SUBTASK 4.10 – ENTERPRISE OPERATIONS, EVENT MONITORING AND MANAGEMENT, PERFORMANCE MONITORING, AND ANALYSIS

The contractor shall provide enterprise operations, event monitoring and management, performance monitoring, and analysis which include, but are not limited to, the following:

- a. Providing services to establish enterprise operations, event monitoring and management, performance monitoring, and analysis services.
- b. Providing centralized operations, monitoring, reporting, management, and analysis of enterprise applications, systems, and core services as well as infrastructure assets to include file servers, email servers, application servers, web server, data delivery, authentication servers, network and storage from all enterprise service providers 24/7/365. Ensuring that monitoring engines are available to all the NCTC personnel.
- c. Monitoring established thresholds, responding to warning and alert messages from the monitoring systems, coordinating corrective action once thresholds are reached to prevent issues from re-occurring, and providing initial troubleshooting to restore services as quickly as possible.
- d. Providing feeds to operations watch staff for situational awareness, responding to escalated incidents and outages (e.g., from the service desk), taking corrective actions to resolve the issue, escalating issues that cannot be resolved within the network operations center, and maintaining/upgrading the supporting network infrastructure and services.

C.5.5 TASK 5 – DATA MANAGEMENT

The contractor shall manage the lifecycle of data within NCTC from the time it is acquired to the time it is removed from NCTC's systems. This includes data transformation and extraction activities, appropriate exploitation and storage of data, implementation and maintenance of data access controls, reporting, and the removal of data in accordance with NCTC's policies and compliance requirements. The contractor shall support the Government in data ingestion,

SECTION J - ATTACHMENTS

management, and other areas of data processing and follow specific guidance provided by the Government related to compliance with authorities and oversight policy for data access loading, minimization, retention, and use.

C.5.5.1 SUBTASK 5.1 – DATA MANAGEMENT AND USE

The contractor shall support bulk data queries (via back-end searches), data science capabilities, and innovative approaches to data exploitation. The contractor shall develop new methodology and visualization capabilities in coordination with the Government.

The contractor shall conduct data transformation and extraction to meet information needs and provide data exposure for analysts in a timely manner. This shall include, but is not limited to, transforming raw data into a usable format, resolving identities from unstructured and structured text, creating networks for social network analysis, enriching results from disparate data sources, helping mission partners evaluate the use and value of new and current datasets, and identifying new selectors for persons of interest.

The contractor shall develop prototype tools and capabilities for baseline integration. This shall include, but is not limited to basic scripting or programing to automate a task regularly performed for mission customers. These scripts or programs can sometimes be enhanced to provide a self-service tool back to the Government, bringing additional value to the mission customer in order to allow team members to focus on more innovative work.

The contractor shall:

- a. Conduct analysis on current data science activities via mission owner and user stakeholder interviews and outreach and make recommendations for strategic application of data science across NCTC.
- b. Research and identify leading practices across the IC, the broader Government, and industry in the development and execution of data science and present findings.
- c. Determine gaps between activities at NCTC and leading practices, and provide recommendations for implementation at NCTC to improve data science-related efforts that align with NCTC mission goals in the areas of Big Data, machine learning, and predictive analytics.
- d. Facilitate discussions between relevant NCTC stakeholder groups based on recommendations and findings in order to formulate an NCTC specific implementation plan for data science.

The contractor shall develop a repeatable methodology for facilitating proofs of concept or rapid prototyping, documenting knowledge capture, and coordinating between affected parties. In support of the proof of concept activities the contractor shall prepare a template for managing and facilitating data science proof of concept efforts based on industry and IC standard practices. Additional requirements include a documented SOP that captures, at a minimum, the activity description, business needs addressed and alignment to strategic goals, evaluation of the effort, and technical considerations. This includes the coordination and documentation of proof of concept or rapid prototyping efforts with all relevant stakeholders across mission area boundaries.

SECTION J - ATTACHMENTS

C.5.5.2 SUBTASK 5.2 – DATA SERVICES, ADMINISTRATION, AND MANAGEMENT

The contractor shall provide data services, administration, and management which include, but are not limited to, the following:

- a. Providing data services, data administration, data management, and “Big Data” support in client/server, virtual machine, Hadoop, and cloud infrastructure environment and/or migrations between these environments.
- b. Providing database installation, configuration, and upgrading database server software and related products, backup and recovery policies and procedures, database implementation, security, optimization, multi-domain operation, and performance management.
- c. Supporting Hadoop, cloud, and other technologies associated with data storage, processing, management, and use.
- d. Supporting the migration/transition of database capability into cloud-based technologies and/or creation of interfaces between classic relational databases and key indexes to cloud-based columnar databases and map reduce index capabilities.

C.5.5.3 SUBTASK 5.3 – ENTERPRISE COMPLIANCE SUPPORT

The contractor shall provide audit support to determine enterprise compliance with all of the NCTC’s current policies and oversight requirements, which include, but are not limited to, the following:

- a. Providing support for data handling obligations under numerous policy and legal authorities, such as Attorney General Guidelines, partner agency information sharing agreements, and security protocols, and assisting the NCTC in maintaining compliance with such requirements.
- b. Designing, testing, and implementing data oversight and auditing solutions for datasets within IT systems.
- c. Monitoring and reporting on the organization’s use of data in accordance with its data access authorities and internal policy, and conducting research and analysis to report on data set usage by dataset, data provider, tool, or compliance requirement in question.
- d. Developing and implementing automated compliance oversight processes for the organization’s use of and access to new datasets and/or emerging technologies.
- e. Conducting technical investigations and audits of IT systems and/or application logs related to data-handling compliance incidents (e.g., late deletions and unauthorized or inappropriate data access) to provide facts regarding access to the data and other issues during the period of non-compliance, and providing investigation results to the appropriate NCTC personnel in a usable and easily understood format.
- f. Providing the NCTC input to periodic interagency reports, reviewing reports for accuracy regarding access to and use of data, and reviewing/reporting on compliance incidents.
- g. Tracking and approving dataset user access requests in accordance with the NCTC SOPs and policies, and providing recommendations for streamlining and updating access procedures.
- h. Formulating methods, documents, and procedures to guide appropriate use of data.

SECTION J - ATTACHMENTS

- i. Updating existing data-handling compliance training courses and materials, developing new materials to reflect changes to data-handling requirements, providing refresher training to the NCTC workforce on the data-handling requirements, and implementing required training.
- j. Tracking and administering the compliance-related training.
- k. Developing and implementing an engagement and communications strategy related to the NCTC's compliance requirements.
- l. Developing a Compliance Innovation Plan (Section F, Deliverable 37) and facilitating discussions between the relevant NCTC stakeholder groups in order to formulate an NCTC specific implementation plan for data-handling compliance.

C.5.6 TASK 6 – PROVIDE ADDITIONAL REACTS RESPONSE SUPPORT (OPTIONAL)

Unpredictable world events require that the contractor shall have the capability to provide additional reach-back, response personnel, and REACTS response support to combat threats and conduct CT activities in pressing situations. The Government reserves the right to exercise additional REACTS response support services at any point during the TO performance, in accordance with the terms and conditions of the contract. The contractor shall provide additional response support for any requirements in Tasks 1 and 3 through 5 that are within the scope of the TO. The contractor shall meet and maintain requirements identified by the NCTC TPOC and the FEDSIM COR during events of contingency or training situations to support directed response planning, exercises, and operations when required by the NCTC.

The additional response support shall not result in a decrease of support to other TO requirements unless approved by the FEDSIM CO and COR.

The following applies to the performance of REACTS additional response support:

- a. The Government will determine the amount of additional REACTS response support required at the time of the situational action matter. Each situational action matter may require a different amount and length of support in order to meet specific requirements.
- b. The contractor shall provide additional REACTS response support in identified situational action matters with the urgency the matter entails. Additional REACTS response support shall be staffed and worked within the NCTC spaces, following the first notification informing the contractor of a request for additional response support.

Once a situational action matter has been declared ended or the additional response support is no longer needed, the contractor shall proceed with an orderly and efficient scale down period NTE 30 days. During the scale down period, the contractor shall fully cooperate and assist the Government with activities closing out the crisis action matter, developing required documentation, transferring knowledge, and documenting lessons learned.